

1 NETWORK DATA PACKET CLASSIFICATION AND DEMULTIPLEXING

2 Abstract

3 The present invention provides methods and apparatus for
4 classifying and demultiplexing packets in a network protocol
5 stack. It provides extendibility for packet processing in the
6 network protocol stack by defining a standard method for adding
7 new functionality. It provides a method to obtain external
8 information, from an application scheduled outside of the
9 forwarding or interrupt context of the kernel, in order to
10 augment packet classification and/or augment packet disposition.
11 In some embodiments, external information augments a criteria of
12 a node in a classification tree with additional information. It
13 presents a way of augmenting which suspends the classification
14 process until an application, scheduled outside of the forwarding
15 or interrupt context of the kernel, completes. The resulting
16 external information is used to augment the packet
17 classification. In some embodiments of the method, the external
18 information includes authentication of an originator of the
19 packet by correlating a tunnel id with a userid, and/or using
20 s/ident for out of band authentication. The classification
21 process enables enforcement of a site policy.